HEWLETT-PACKARD COMPANY Intellectual Property Administration P.O. Box 272400 Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200401716-1

IN THE

UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): John APOSTOLOPOULOS et al. Confirmation No.: 8407

Application No.: 10/810,025 Examiner: Daniel L. HOANG

Filing Date: 03/26/2004 Group Art Unit: 2136

Title: METHODS AND SYSTEMS FOR GENERATING TRANSCODABLE ENCRYPTED CONTENT

Mail Stop Appeal Brief-Patents Commissioner For Patents PO Box 1450 Alexandria, VA 22313-1450

RESPONSE TO NON-COMPLIANT APPEAL BRIEF

Transmitted her on 10/29/2008		is the Appeal	Brief in	this	application v	with resp	ect to	the Notice o	f Non-Co	omplia	ant Appeal Brief mailed
				(cor	mplete (a) o	r (b) as	applic	cable)			
The proceeding	s here	ein are for a pa	atent app	plica	tion and the	provisio	ns of	37 CFR 1.13	6(a) app	ly.	
(a) Applicant months cl			tension	of ti	me under 3	7 CFR [^]	1.136	(fees: 37 CF	FR 1.17(a)-(d)) for the total number of
		1st Month \$120	ļ		2nd Month \$460			3rd Month \$1050			4th Month \$1640
☐ The exter	nsion	fee has alread	y been t	filed	in this appli	cation.					
(b) Applicant the possib	belie oility t	ves that no ex hat applicant h	tension nas inad	of tir verte	me is require ently overloo	ed. Howe ked the	ever, t need	his condition for a petition	al petitio and fee	n is b for ex	eing made to provide for xtension of time.
Additionally plea	any f	fees required harge any fee	or cred s to Dep	lit a oosit	ny over pa	yment to 3-2025 u	Dep	osit Áccoun 37 CFR 1.16	t 08-202 through	25 pu 1.21	ndency of this application irsuant to 37 CFR 1.25 inclusive, and any othen his sheet is enclosed.
								spectfully subrohn APOSTC		ILOS	et al.
							Ву_	/John P. Wa	igner, Jr.	./	
								John P. Wa	gner, Jr.		
	Attorney/Agent for Applicant(s))
							F	Reg No. : 35,3	398		

Date: 12/01/2008

Telephone: 408-377-0500

Rev 10/05 (AplBrief)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant: APOSTOLOPOULOS et al. Patent Application

Application No.: 10/810,025 Group Art Unit: 2136

Filed: March 26, 2004 Examiner: Hoang, Daniel L.

For: METHODS AND SYSTEMS FOR GENERATING TRANSCODABLE

ENCRYPTED CONTENT

APPEAL BRIEF

200401716-1 Group Art Unit: 2136

Table of Contents

	<u>Page</u>
Real Party in Interest	1
Related Appeals and Interferences	2
Status of Claims	3
Status of Amendments	4
Summary of Claimed Subject Matter	5
Grounds of Rejection to Be Reviewed on Appeal	8
Argument	9
Conclusion	15
Appendix – Clean Copy of Claims on Appeal	16
Appendix – Evidence Appendix	23
Annendix – Related Proceedings Annendix	24

200401716-1 Serial No.: 10/810,025 Group Art Unit: 2136

I. Real Party in Interest

The assignee of the present application is Hewlett-Packard Development Company, L.P.

200401716-1 Group Art Unit: 2136

II. Related Appeals and Interferences

None. There are no related appeals or interferences known to the Appellants.

200401716-1 Group Art Unit: 2136

III. Status of Claims

Claims 1-34 are pending. Claims 1-34 are rejected. This Appeal involves Claims 1-34.

200401716-1 Group Art Unit: 2136

IV. Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Office Action mailed April 14, 2008, <u>has not been filed</u>.

200401716-1 Group Art Unit: 2136

V. Summary of Claimed Subject Matter

Independent Claims 1, 12 and 24 of the instant application pertain to embodiments

associated with generating and transcoding transcodable encrypted content that comprises

independently processable components.

As recited in Claim 1, "[a] method for generating transcodable encrypted content that

comprises independently processable components" is described. This embodiment is depicted

at least in FIG. 1 and FIG. 4. "FIG. 4 is a flowchart 400 of the steps performed in a method

for generating transcodable encrypted content (e.g., 104 of FIG. 1) according to one

embodiment of the present invention" (page 15, lines 20-22). "At step 401, transcodable

content (e.g., 101 of FIG. 1) that includes independently processable components is accessed"

(page 15, lines 29-30). "At step 403, at least one of the independently processable

components (e.g., 101a-101f of FIG. 1) that constitute the transcodable content (e.g., 101 of

FIG. 1) is encrypted to provide transcodable encrypted content (e.g., 104 of FIG. 1) that has

independently processable components (e.g., 101a-101f in FIG. 1) which are independently

decryptable. The encryption is performed using an encryption scheme that utilizes non-

repeating identifiers that uniquely correspond to the independently processable components

(e.g., 101a-101f of FIG. 1). The transcodable encrypted content (e.g., 104 of FIG. 1) that is

provided is transcodable without requiring knowledge of the encryption scheme that is used"

(page 16, lines 6-15).

As recited in Claim 12, "[a] method for transcoding transcodable encrypted content

that comprises independently processable components" is described. This embodiment is

depicted at least in FIG. 1 and FIG. 5. "FIG. 5 is a flowchart of the steps performed in a

200401716-1

Group Art Unit: 2136

Serial No.: 10/810,025

method for transcoding transcodable encrypted content (e.g., 104 of FIG. 1) according to one embodiment of the present invention" (page 17, lines 13-14). "At step 501, transcodable encrypted content (e.g., 104 of FIG. 1) that has been encrypted using non-repeating identifiers is accessed. The non-repeating identifiers uniquely correspond to independently processable components (e.g., 101a-101f of FIG. 1) (of which the transcodable content is constituted) such that the independently processable components (e.g., 101a-101f of FIG. 1) are independently decryptable" (page 17, lines 23-28). "At step 503, the transcodable encrypted content (e.g., 104 of FIG. 1) is transcoded without requiring knowledge of the encryption scheme used to encrypt at least one of its independently processable components (e.g., 101a-101f of FIG. 1)" (page 18, lines 6-9).

As recited in Claim 24, "[a] transcodable encrypted content generator for generating transcodable encrypted content that comprises independently processable components" is described. This embodiment is depicted at least in FIG. 1, FIG. 2 and FIG. 3. "Accessor 201 accesses transcodable content that includes independently processable components (e.g., 101a-101f in FIG. 1) from a source of transcodable content (e.g., server, storage etc.)" (page 10, lines 5-7). "Encryptor 202 accesses transcodable content 101 supplied by accessor 201 and encrypts at least one of the independently processable components 101a-101f that constitute transcodable content 101. According to one embodiment, this manner of encryption provides transcodable encrypted content 104 that is comprised of independently processable components which are also independently decryptable" (page 10, lines 13-18). "Referring to FIG. 3, non-repeating identifier engine 203 produces non-repeating identifiers that uniquely correspond to the independently processable components 101a-101f that constitute the transcodable content" (page 12, lines 16-18). "Output 211 outputs transcodable encrypted

200401716-1 Group Art Unit: 2136

content 104 that can be supplied to downstream sources (e.g., transcoder, client, etc.).

According to one embodiment, the transcodable encrypted content 104 which is output by output 211 can be transcoded by downstream sources without requiring knowledge of the encryption scheme that is used by encryptor 202" (page 11, lines 26-30).

200401716-1 Group Art Unit: 2136

VI. Grounds of Rejection to Be Reviewed on Appeal

1. Claims 1-34 are rejected under 35 U.S.C. §103(a) as being unpatentable over 6,963,972 by Chang et al., hereinafter referred to as "Chang," in view of "Recommendation for Block Cipher Modes of Operation – Methods and Techniques" by Dworkin, hereinafter referred to as "Dworkin."

200401716-1 Group Art Unit: 2136

VII. Argument

1. Whether Claims 1-34 are unpatentable under 35 U.S.C. §103(a) by Chang in view of Dworkin.

According to the Final Office Action mailed April 14, 2008, Claims 1-34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chang in view of Dworkin. Appellants have reviewed Chang and Dworkin and respectfully submit that the claimed embodiments are patentable over the combination of Chang and Dworkin, for at least the following rationale.

Independent Claim 1 recites, in part, "accessing transcodable content that comprises independently processable components to be encrypted; and encrypting at least one of said independently processable components" (emphasis added). Independent Claims 12 and 24 recite similar embodiments. Claims 2-11, 13-23 and 25-34 depend on Claim 1, 12 or 24 and also include these embodiments.

"As reiterated by the Supreme Court in *KSR*, the framework for the objective analysis for determining obviousness under 35 U.S.C. 103 is stated in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). Obviousness is a question of law based on underlying factual inquiries" including "[a]scertaining the differences between the claimed invention and the prior art" (MPEP 2141(II)). "In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious" (emphasis in original; MPEP 2141.02(I)). Appellants note that "[t]he prior art reference (or references when combined) need not teach or suggest all the claim limitations, however, Office personnel must explain why the difference(s) between the prior art and the claimed

200401716-1 Group Art Unit: 2136

invention would have been obvious to one of ordinary skill in the art" (emphasis added; MPEP 2141(III)).

Furthermore, Appellants submit that "[a] prior art reference must be considered in its entirety, i.e., as a <u>whole</u>, including portions that would lead away from the claimed invention" (emphasis in original; MPEP 2141.03(IV)).

Appellants respectfully submit that Chang does not teach, describe or suggest "accessing transcodable content that comprises <u>independently processable components</u> to be encrypted; and encrypting at least one of said <u>independently processable components</u>" (emphasis added) as claimed, as asserted in the Office Action mailed April 14, 2008. In contrast, Appellants understand Chang to disclose that the processing of component is <u>dependent</u> on the associated metadata. In particular, Appellants understand Chang to disclose that the metadata is used to process a component, thereby introducing dependencies into the processing of the components.

Appellants understand Chang to describe a method and apparatus for networked information dissemination through secure transcoding whereby metadata information is added to data components, the combined metadata information and data components are encrypted, and additional metadata is added to the encrypted metadata and data components (col. 9, lines 24-26, and col. 10, lines 24-27). In particular, Chang discloses that the "[c]lear-text metadata preferably provides a semantic understanding of the absolute or relative importance/priority of the components with respect to each other, thereby facilitating the transcoding process" (emphasis added; Abstract). In other words, Appellants understand Chang to disclose that the processing of a component is dependent on the associated metadata, and therefore the

200401716-1 Group Art Unit: 2136

components are not "independently processable components" as claimed. Furthermore, Appellants understand that the components of Chang are not transcodable without the associated metadata. Therefore, Appellants respectfully submit that the transcoding of a component relies on its associated metadata.

Chang recites that "[e]ach of these components is also preferably annotated with a metadata header, including but not limited to component identification fields and information regarding the relative importance/priority of the particular component" (emphasis added; col. 4, lines 1-5). Specifically, "[t]he transcoding proxy receives the multiple messages corresponding to each component and inspects the metadata header of each message to determine which encrypted components should be selectively filtered" (emphasis added; col. 4, lines 12-15). As such, Appellants understand that the transcoding of each component is dependent on the metadata for that component.

With reference to Figure 10, Chang discloses a transcoding process that determines which components to filter utilizing the metadata. Chang recites "[u]sing the information provided in the extracted metadata header, the transcoding proxy selectively manipulates 1003 the received components, such as by determining which encrypted components or component portions of the received message(s) to filter" (emphasis added; col. 10, lines 58-62). "The metadata headers, or other suitable equivalent annotating data, accompanying each message preferably furnish the transcoding proxy with sufficient semantic understanding of the components to make an informed determination concerning which components to filter and which components to send to the client device" (emphasis added; col. 11, lines 28-33). In particular, Appellants understand Chang to disclose that the processing of one component is

200401716-1 Group Art Unit: 2136

<u>dependent</u> on its associated metadata, and therefore the components are not "independently processable components" as claimed.

Therefore, Appellants respectfully submit that Chang does not teach, describe or suggest "accessing transcodable content that comprises independently processable components to be encrypted; and encrypting at least one of said independently processable components" (emphasis added) as claimed. Moreover, by disclosing that components are processed by inspecting the metadata headers, Appellants respectfully submit that Chang teaches away from "accessing transcodable content that comprises independently processable components to be encrypted; and encrypting at least one of said independently processable components" (emphasis added) as claimed. In other words, by disclosing that the processing of one component is dependent on its associated metadata, Appellants respectfully submit that Chang teaches away from the claimed embodiments of "independently processable components."

Appellants note the Response to Arguments of the Final Office Action mailed April 14, 2008, asserts that the "[t]he Chang reference cites at col. 3, lines 65-67 and col. 4, lines 1-11, that the source data is subdivided into multiple data components. These components themselves are processed independently from each other. Whether or not they are annotated with metadata headers or later assembled into messages with comprise clear-text data is irrelevant as to how they are processed in relation to each other. The components themselves are encrypted and decrypted independently" (emphasis added; Final Office Action mailed April 14, 2008; page 2, last paragraph). Appellants respectfully disagree.

200401716-1 Group Art Unit: 2136

Appellants respectfully maintain that the components of Chang are not transcodable without the associated metadata. Chang recites that "[c]lear-text metadata preferably provides a semantic understanding of the absolute or relative importance/priority of the components with respect to each other, thereby facilitating the transcoding process" (Abstract). By disclosing that metadata includes information describing the relative relationship of components for transcoding, Appellants respectfully submit that Chang discloses that the components are not independently processable.

Moreover, Appellants understand the statement in Final Office Action that "[t]he components themselves are encrypted and decrypted independently" as supporting the assertion that the component of Chang are independently processable. Appellants respectfully submit that the claimed embodiments recite "accessing transcodable content that comprises independently processable components to be encrypted" (emphasis added). In particular, Appellants submit that the claimed "independently processable components" are independently processable without encryption. Therefore, Appellants submit that the asserted independent encryption or decryption of Chang does not teach, describe or suggest "independently processable components" as claimed.

Furthermore, Appellants respectfully submit that Dworkin does not overcome the shortcomings of Chang. Appellants understand Dworkin to describe "confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm" (page v, Abstract). In particular, Appellants respectfully submit that Dworkin does not teach, describe or suggest "accessing transcodable content that comprises <u>independently processable</u>

200401716-1 Group Art Unit: 2136

<u>components</u> to be encrypted; and encrypting at least one of said <u>independently processable</u> components" (emphasis added) as claimed.

In view of the combination of Chang in view of Dworkin not satisfying the requirements of a *prima facie* case of obviousness, Appellants respectfully submit that independent Claims 1, 12 and 24 overcome the rejection under 35 U.S.C. § 103(a), and that these claims are thus in a condition for allowance. Appellants respectfully submit the combination of Chang in view of Dworkin also does not teach or suggest the additional claimed features of the present invention as recited in Claims 2-11 that depend from independent Claim 1, Claims 13-23 that depend from independent Claim 12, and Claims 25-34 that depend from independent Claim 24. Therefore, Appellants respectfully submit that Claims 2-11, 13-23 and 25-34 also overcome the rejection under 35 U.S.C. § 103(a), and are in a condition for allowance as being dependent on an allowable base claim.

200401716-1 Group Art Unit: 2136

Conclusion

Appellants believe that pending Claims 1-34 are patentable over the cited art. As such, Appellants respectfully request that the rejections of Claims 1-34 be reversed.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted, WAGNER BLECHER LLP

Dated: December 1, 2008 /John P. Wagner, Jr./

John P. Wagner, Jr. Registration No. 35,398 123 Westridge Drive Watsonville, CA 95076

Phone: (408) 377-0500 Facsimile: (831) 722-2350

200401716-1 Group Art Unit: 2136

VIII. Appendix - Clean Copy of Claims on Appeal

1. A method for generating transcodable encrypted content that comprises

independently processable components, said method comprising:

accessing transcodable content that comprises independently processable components

to be encrypted; and

encrypting at least one of said independently processable components to provide

independently processable components which are independently decryptable, said encrypting

performed using an encryption scheme that utilizes non-repeating identifiers that uniquely

correspond to said independently processable components, wherein said transcodable

encrypted content is transcodable without requiring knowledge of said encryption scheme.

2. The method as recited in Claim 1 wherein said independently processable

components comprise components that are independently decodable and independently

authenticatable.

3. The method as recited in Claim 1 wherein said encryption scheme comprises

applying block ciphers in stream cipher mode.

4. The method as recited in Claim 1 wherein said encryption scheme comprises

counter (CTR) mode stream cipher encryption.

5. The method as recited in Claim 1 wherein said encryption scheme comprises

encrypting a counter to generate a keystream which is logically combined with plaintext to

generate ciphertext.

200401716-1

Group Art Unit: 2136

Serial No.: 10/810,025

6. The method as recited in Claim 1 wherein said encryption scheme utilizes non-

repeating identifiers which are non-repeating counter values.

7. The method as recited in Claim 1 wherein said encryption scheme comprises

performing several encryptions in parallel.

8. The method as recited in Claim 1 wherein differentiating metadata that

corresponds to said independently processable components is used as an input to said

encryption.

9. The method as recited in Claim 1 wherein said transcodable encrypted content

has information associated with it to direct transcoding.

10. The method as recited in Claim 1 said transcodable encrypted content

comprises respective components that have respective encryption keys, wherein said

respective encryption keys are related to a root encryption key.

11. The method as recited in Claim 1 wherein said encryption scheme is selected

from the group consisting of a block cipher used in output feedback (OFB) mode, RC4,

SEAL, and WAKE.

12. A method for transcoding transcodable encrypted content that comprises

independently processable components comprising:

200401716-1

Group Art Unit: 2136

Serial No.: 10/810,025

accessing transcodable encrypted content that has been encrypted using non-repeating

identifiers that uniquely correspond to said independently processable components such that

said independently processable components are independently decryptable, and

transcoding said transcodable encrypted content without requiring knowledge of the

encryption scheme used to encrypt said independently processable components.

13. The method as recited in Claim 12 wherein said independently processable

components comprise components that are independently decodable and independently

authenticatable.

14. The method as recited in Claim 12 wherein said encryption scheme comprises

applying block ciphers in stream cipher mode.

15. The method as recited in Claim 12 wherein said encryption scheme comprises

counter (CTR) mode stream cipher encryption.

16. The method as recited in Claim 12 wherein said encryption scheme comprises

encrypting a counter to generate a keystream which is logically combined with plaintext to

generate ciphertext.

17. The method as recited in Claim 12 wherein said encryption scheme utilizes

non-repeating identifiers which are non-repeating counter values.

200401716-1

Serial No.: 10/810,025

Group Art Unit: 2136

18. The method as recited in Claim 12 wherein said encryption scheme comprises

performing several encryptions in parallel.

19. The method as recited in Claim 12 wherein differentiating metadata that

corresponds to said independently processable components is used as an input to said

encryption.

20. The method as recited in Claim 12 wherein said transcoding produces

transcodable encrypted content that is smaller in size than the transcodable encrypted content

that is accessed.

21. The method as recited in Claim 12 wherein said transcodable encrypted

content has information associated with it to direct transcoding.

22. The method as recited in Claim 12 said transcodable encrypted content

comprises respective components that have respective encryption keys, wherein said

respective encryption keys are related to a root encryption key.

23. The method as recited in Claim 12 wherein said encryption scheme is selected

from the group consisting of a block cipher used in output feedback (OFB) mode, RC4,

SEAL, and WAKE.

200401716-1

Serial No.: 10/810,025

19

Group Art Unit: 2136

A transcodable encrypted content generator for generating transcodable 24.

encrypted content that comprises independently processable components, said transcodable

encrypted content generator comprising:

an accessor for accessing transcodable encrypted content that comprises independently

processable components to be encrypted; and

an encryptor coupled to said accessor for encrypting at least one of said independently

processable components to provide independently processable components which are

independently decryptable, said encryptor further comprising:

a non-repeating identifier engine that produces non-repeating identifiers that

uniquely correspond to said independently processable components; and

an output coupled to said encryptor, said output outputting transcodable encrypted

content which is transcodable without requiring knowledge of an encryption scheme used by

said encryptor to encrypt said at least one of said independently processable components.

25. The transcodable encrypted content generator of Claim 24 wherein said

accessor is configured to access independently processable components that are independently

decodable and independently authenticatable.

26. The transcodable encrypted content generator of Claim 24 wherein said

encryptor comprises:

a block-stream cipher engine that applies block ciphers in stream cipher mode.

27. The transcodable encrypted content generator of Claim 24 wherein said

encryptor comprises:

200401716-1

Serial No.: 10/810,025

Group Art Unit: 2136

a counter (CTR) mode stream cipher encryptor.

28. The transcodable encrypted content generator of Claim 24 wherein said

encryptor further comprises:

a keystream engine which encrypts a counter to generate a keystream; and

a combiner coupled to said keystream engine, said combiner configured to logically

combine said keystream with plaintext to generate ciphertext.

29. The transcodable encrypted content generator of Claim 24 wherein said non-

repeating identifier engine is configured to produce non-repeating identifiers which are non-

repeating counter values.

30. The transcodable encrypted content generator of Claim 24 wherein said

encryptor is configured to perform several encryptions in parallel.

31. The transcodable encrypted content generator of Claim 24 wherein said encryptor

further comprises:

a differentiator which accesses differentiating metadata that corresponds to said

independently processable components and associates the differentiating metadata with the

independently processable components.

32. The transcodable encrypted content generator of Claim 24 wherein said

transcodable encrypted content has information associated with it to direct transcoding.

200401716-1

Group Art Unit: 2136 Serial No.: 10/810,025

33. The transcodable encrypted content generator of Claim 24 wherein said transcodable encrypted content comprises respective components that have respective encryption keys, wherein said respective encryption keys are related to a root encryption key.

34. The transcodable encrypted content generator of Claim 24 wherein said encryption scheme is an encryption scheme selected from the group consisting of a block cipher used in output feedback (OFB) mode, RC4, SEAL, and WAKE.

200401716-1 Group Art Unit: 2136

IX. Evidence Appendix

None. No evidence is herein appended.

200401716-1 Group Art Unit: 2136

X. Related Proceedings Appendix

None. No related proceedings are herein appended.

200401716-1 Group Art Unit: 2136